Association for Information Systems
AIS Electronic Library (AISeL)

MCIS 2016 Proceedings

Mediterranean Conference on Information Systems (MCIS)

2016

# Users' Attitudes on Mobile Devices: Can Users' Practices Protect their Sensitive Data?

Ioannis Stylios
*University of the Aegean*, istylios@aegean.gr

Spyros Kokolakis
*University of the Aegean*, sak@aegean.gr

Olga Thanou
*University of Athens*, o.thanou@hotmail.com

Sotirios Chatzis
*Cyprus University of Technology*, sotirios.chatzis@eecei.cut.ac.cy

# USERS' ATTITUDES ON MOBILE DEVICES: CAN USERS' PRACTICES PROTECT THEIR SENSITIVE DATA?

*Completed Research*

Stylios, Ioannis, University of the Aegean, Samos, Greece, istylios@aegean.gr

Kokolakis, Spyros, University of the Aegean, Samos, Greece, sak@aegean.gr

Thanou, Olga, University of Athens, Athens, Greece, o.thanou@hotmail.com

Chatzis, Sotirios, Cyprus University of Technology, Cyprus, sotirios.chatzis@eecei.cut.ac.cy

## Abstract

*Smartphones are the most popular personal electronic devices. They are used for all sorts of purposes, from managing bank accounts to playing games. As smartphone apps and services proliferate, the amount of sensitive data stored on or processed by handheld devices rise as well. This practice entails risks, such as violating users' privacy, stealing users' identities, etc. Particularly, stealing an unlocked device grants full access to sensitive data and applications. In this survey, we examine whether users adopt some basic practices to protect their sensitive personal data themselves, or is there a need to further strengthen their protection? Our statistical analysis assesses smartphone users' security attitudes and practices among different age groups. Finally, we investigate the factors that affect the attitude of users with respect to their practices for the protection of personal data.The results of this study, show that while many smartphone users do take some security precautions, a high percentage (24%) of them still ignores security and privacy risks. In addition, 19,1 % of users do not follow any practices to protect their PINs and Passwords.*

*Keywords: Mobile Phones, Privacy Risk, Users Attitudes, Survey.*

# 1 Introduction

The wealth of services that were made available over the last few years including access to emails, social media, banking, etc. has led to the rise of the amount of sensitive data stored on or processed by handheld devices (Androulidakis et al., 2014). Users choose easy to remember passwords, for all their tasks; thus, the level of protection decreases significantly (Androulidakis et al., 2009). Even though handheld devices require frequent user authentication, an attacker could gain access to the device after the successful authentication of the legitimate user, and misuse all sensitive data, (Bo et al., 2014). In addition, despite the fact that mobile phone's security safeguards have been increased during the last years, users don't take the necessary measures to avoid a possible unauthorized access and sensitive data retrieval from their mobile phone (Clarke and Furnell, 2005). Finally, there is a plethora of recent articles, which indicates that password authentication is not appropriate for mobile devices (Dillman, 1999; Frank et al., 2013).

In this survey, we examine if the users adopt some basic practices to protect their sensitive personal data or if there is a need to further strengthen their protection. To this end, we used an original questionnaire, created for the specific needs of this survey. Our main variable is age, as we aim to evaluate the significance of age in users' security attitudes and practices. The survey sample includes 204 students, employees, and faculty of the University of Athens and the University of the Aegean.

Our survey aims to address three main research questions:

1. What are users' security attitudes on mobile devices?
2. Are users' practices sufficient to protect their sensitive data?
3. Is there a need to strengthen the protection of users' personal data?

Finally, we seek the factors that affect users' attitudes in relation to the practices they follow so as to protect their personal data. To achieve this we investigated, through statistical analysis, whether age and gender relate to users' practices for the protection of their personal data. Our survey examines three main research hypotheses:

1. H1: Age correlates to users' practices concerning the storage of important passwords on their mobile phone.
2. H2: Age correlates to the users' practices concerning the storage of sensitive personal data on their mobile (photographs / videos /voice recordings etc.).
3. H3: Gender correlates to the users' practices concerning the sharing of their PIN with third persons.

The above hypotheses are important because they examine the correlation of *age* (1, 2), *gender* (3) and security practices. This analysis is also important for the reason that in the literature we find conflicting views with regard to the aforementioned correlations. For example, in some cases young people are considered "frivolous", while in other cases they are considered "good and knowledgeable users of technology and, therefore, able to protect themselves" (Blank et al., 2014; Miltgen and Peyrat-Guillard, 2014). The same applies to gender as well (Jones and Heinrichs, 2012).

# 2 Related work

In this section we review recent publications that are relevant to the subject of our survey.

Clarke and Furnell (2005) conducted a survey of 297 mobile subscribers, with the aim to assess their use of mobile devices, their use of current authentication methods, and their attitudes towards future security options. The findings revealed that the majority of the respondents make significant use of their devices, with clear demands for protection against unauthorized use. However, the use of current

PIN-based authentication was marked as problematic, with a third of the respondents indicating that they do not use it at all, and further issues being reported amongst those that do. In view of this, 83% of the respondents stated that they are willing to accept some form of biometric authentication on their device.

Ahern et al. (2007) used context-aware camera phone devices to examine privacy decisions in mobile and online photo sharing. Through data analysis on a corpus of privacy decisions and associated context data from a real-world system, they identified relationships between location of photo capture and photo privacy settings. Their data analysis led to further questions which they investigated through a set of interviews with 15 users. The interviews revealed common themes in privacy considerations, namely: *security, social disclosure, identity* and *convenience*.

Kurkovsky and Syta (2010) presented the results of a survey of over 330 young people, aged 18 to 25, namely known as digital natives. They aimed to assess their use of mobile technology, their attitudes regarding security and privacy as it relates to mobile phones, as well as their perceptions of different ways how security and privacy could be improved in future mobile devices. Despite a commonly held belief that digital natives are technologically savvy, their self-assessment did not appear to support this statement. Furthermore, despite the respondents' awareness of various threats to security and privacy, very few of them actually took any concrete steps to protect their devices from unauthorized access.

Chin et al. (2012) conducted a user study involving 60 smartphone users. First, they interviewed users about their willingness to perform certain tasks on their smartphones to test the hypothesis that people currently avoid using their phones due to privacy and security concerns. Second, they analyzed why and how they select applications, which provided information about how users decide to trust applications.

Keith et al. (2013) proposed and tested an experimental methodology designed to replicate real perceptions of privacy risk and capture the effects of actual information disclosure decisions. Subsequently, they reported the results of a controlled experiment involving a sample of 1025 consumers in a range of ages, levels of education, and employment experience. Based on their methodology, they found that only a weak, albeit significant, relationship exists between information disclosure intentions and actual disclosure. In addition, this relationship is heavily moderated by the consumer practice of disclosing false data.

Jones and Heinrichs (2012) presented a survey of business students with regard to their smartphone security practices. The results of this survey showed students to be lax in their smartphone security with men more willing to engage in risky behaviors than women. The main limitation to this research is that the generalizability of the study is limited because the subject pool only included students in business classes at one university.

By summarizing the related work in some cases the young are considered as good and knowledgeable users of technology and, therefore, able to protect themselves, while in other cases they are not, Blank et al. (2014); (Miltgen and Peyrat-Guillard, 2014). The same applies to the gender as well (Jones and Heinrichs, 2012). Regarding to the various issues of Privacy on Mobile Devices they support that the password is not sufficient for the protection of mobile devices (Clarke and Furnell, 2005; Ahern et al., 2007; Kurkovsky and Syta, 2010; Chin et al., 2012; Keith et al., 2013). Also, Aviv et al. (2010) proved that mobile devices are vulnerable to smudge attacks. Finally, Clarke et al. (2002; 2005) and Karatzouni et al. (2007) showed that users are willing to adopt alternative methods of authentication such as biometrics in order to protect their privacy on their devices.

# 3 Methodology

Our survey was conducted using a structured questionnaire, with a total of 204 participants that were requested to complete it anonymously and voluntarily. The target group of the survey is University of Aegean and University of Athens students, professors, and employees.

A very useful evaluation method for surveying user's practices is the use of multiple-choice questionnaires (Dillman, 1999). This method was selected from other alternatives because it is more accurate and has a bigger degree of participation from the respondents.

The questionnaire is original and created for the needs of the specific survey. It consists of six subsections and is formed as follows:

1. Demographics
2. Storage Practices
3. PIN Practices
4. Device Protection

We tried to formulate our questions in a fully understood way, in order to be answered and filled correctly. The parts of the questionnaire follow a logical continuity and are clearly distinct, since we have used headings that indicate each group of questions.

From the tests presented above we eventually ended up using the Kolmogorov–Smirnov and the Kruskal – Walis tests. We used the Kolmogorov–Smirnov test to see if we have a normal distribution so as to either use a parametric or a non-parametric test. Since we don't have a normal distribution, in the cases we examined, and we had more than two groups to check, we applied the non-parametric Kruskal – Walis test ($p<0.05$) on SPSS. We examine if there is a statistically significant difference between the age groups in correlation to the variables.

# 4 Survey Results

In the following sections, survey results are presented in detail and an analysis and discussion of every issue is made.

### 4.1.1 Demographics

The gender of the participants were 55,9% males and 44,1% females. Most of them were studying Applied Sciences (52.9%), 18.2 studied Theoretical Sciences and 28.9% Technological Sciences. In the following table we can see the age groups of the participants.

| Age_groups | Frequency | Percent |
|---|---|---|
| 18-24 | 89 | 43,6 % |
| 25-30 | 37 | 18,1 % |
| 31-35 | 21 | 10,3 % |
| 36-40 | 30 | 14,7 % |
| 41-45 | 15 | 7,4 % |
| 46-50 | 12 | 5,9 % |
| Total | 204 | 100,0 % |

*Table 3. Group of Ages*

### 4.1.2 Storage Practices

In this subsection of questions the users answered about their storage practices as follows:

- Do you store sensitive personal data on your mobile device? (e.g. photographs / videos / etc.).

| Age_groups | No | Yes |
|---|---|---|
| 18-24 | 15,7% | 84,3% |
| 25-30 | 16,2% | 83,8% |
| 31-35 | 9,5% | 90,5% |
| 36-40 | 10,0% | 90,0% |
| 41-45 | 46,7% | 53,3% |
| 46-50 | 41,7% | 58,3% |
| Total | 18,1% | 81,9% |

*Table 6. Sensitive personal data storage*

As we can see, in the results of table 6, 81,9% of the users do store sensitive personal data on their mobile devices such as: photographs, videos, conversations' recordings, etc. A small percentage of the users, 18.1%, do not stores important sensitive personal data on their mobile devices.

- Do you store passwords of critical applications on your mobile device? (bank PINs, etc.)

| Age_groups | No | Yes, encrypted | Yes, without encryption |
|---|---|---|---|
| 18-24 | 74,2% | 12,4% | 13,5% |
| 25-30 | 81,1% | 2,7% | 16,2% |
| 31-35 | 76,2% | 9,5% | 14,3% |
| 36-40 | 50,0% | | 50,0% |
| 41-45 | 86,7% | 13,3% | |
| 46-50 | 66,7% | 8,3% | 25,0% |
| Total | 72,5% | 8,3% | 19,1% |

*Table 7. Passwords of critical applications storage*

As we can see in table 7, 72,5% of the users do not store passwords of critical applications on their mobile devices. A great percentage of the users, 19.1, stores important passwords such as bank PINs' etc. without encryption. The percentage that actually stores important passwords on their device encrypted is only 8,3%.

### 4.1.3 PIN practices

In this subsection of questions the users answered about the password practices they apply. The results are as follows:

- Have you activated the PIN question on your SIM card?

| Age_groups | No | Yes |
|---|---|---|
| 18-24 | 23,6% | 76,4% |
| 25-30 | 13,5% | 86,5% |
| 31-35 | 14,3% | 85,7% |
| 36-40 | 40,0% | 60,0% |
| 41-45 | 40,0% | 60,0% |
| 46-50 | 33,3% | 66,7% |
| Total | 25,0% | 75,0% |

*Table 8. PIN question on SIM card*

We observe that 75% has activated the PIN question on their SIM card. But, as we can see in table 9 the vast majority (85%) never changes their PIN.

- How often do you change the PIN question on your mobile device?

| Age_groups | Never | Once a year | Twice a year | 3 times a year | More often |
|---|---|---|---|---|---|
| 18-24 | 80,9% | 16,9% | | | 2,2% |
| 25-30 | 91,9% | 8,1% | | | |
| 31-35 | 90,5% | 9,5% | | | |
| 36-40 | 86,7% | 6,7% | 3,3% | 3,3% | |
| 41-45 | 93,3% | | | | 6,7% |
| 46-50 | 83,3% | | | | 16,7% |
| Total | 85,8% | 10,8% | 0,5% | 0,5% | 2,5% |

*Table 9. Frequency of change of the PIN question*

- Do you have a PIN on your mobile's phone Screen-Saver and how often do you change it?

| Age_groups | Once a year | Twice a year | 3 times a year | I do not know if it has such an option | does not have such an option | More often | Never |
|---|---|---|---|---|---|---|---|
| 18-24 | 14,6% | 11,2% | 7,9% | 9,0% | 6,7% | 15,7% | 34,8% |
| 25-30 | 16,2% | 2,7% | 5,4% | 2,7% | 13,5% | 10,8% | 48,6% |
| 31-35 | 9,5% | | | 4,8% | 4,8% | 4,8% | 76,2% |
| 36-40 | 10,0% | 6,7% | | 43,3% | | 3,3% | 36,7% |
| 41-45 | | | | 40,0% | 6,7% | | 53,3% |
| 46-50 | 8,3% | | 8,3% | 41,7% | 16,7% | | 25,0% |
| Total | 12,3% | 6,4% | 4,9% | 16,7% | 7,4% | 9,8% | 42,6% |

*Table 10.* PIN *question on mobile's phone Screen-Saver*

- Do you protect sensitive applications with a PIN or touch gestures?

| Age_groups | No | Yes |
|---|---|---|
| 18-24 | 69,7% | 30,3% |
| 25-30 | 78,4% | 21,6% |
| 31-35 | 61,9% | 38,1% |
| 36-40 | 90,0% | 10,0% |
| 41-45 | 93,3% | 6,7% |
| 46-50 | 83,3% | 16,7% |
| Total | 76,0% | 24,0% |

*Table 11. Protection of sensitive applications with a PIN or touch gestures*

- How often do you change the PIN on your cash card?

| Age_groups | 3 times a year | More often | Never | Once a year | Twice a year |
|---|---|---|---|---|---|
| 18-24 | 3,4% | 3,4% | 82,0% | 7,9% | 3,4% |
| 25-30 | | 5,4% | 73,0% | 18,9% | 2,7% |
| 31-35 | | 9,5% | 66,7% | 19,0% | 4,8% |
| 36-40 | 3,3% | 3,3% | 90,0% | | 3,3% |
| 41-45 | | | 80,0% | 20,0% | |
| 46-50 | | 25,0% | 50,0% | 16,7% | 8,3% |
| Total | 2,0% | 5,4% | 77,9% | 11,3% | 3,4% |

*Table 12. Frequency of change of the PIN on cash card*

- Do you give your PIN to third persons?

| Age_groups | Yes | No |
|---|---|---|
| 18-24 | 20,2% | 79,8% |
| 25-30 | 21,6% | 78,4% |
| 31-35 | 9,5% | 90,5% |
| 36-40 | 40,0% | 60,0% |
| 41-45 | 20,0% | 80,0% |
| 46-50 | 25,0% | 75,0% |
| Total | 22,5% | 77,5% |

*Table 13. Do you give your PIN?*

### 4.1.4 Device Protection

In this group of questions users answered about how careful they are with their device. The results are as follows:

- Have you ever lost your phone or has it ever been stolen?

| Age_groups | Twice | Once | Never | More | 3 times |
|---|---|---|---|---|---|
| 18-24 | 1,1% | 22,5% | 76,4% | | |
| 25-30 | 5,4% | 18,9% | 73,0% | | 2,7% |
| 31-35 | 14,3% | 19,0% | 66,7% | | |
| 36-40 | 10,0% | 30,0% | 56,7% | 3,3% | |
| 41-45 | | 6,7% | 93,3% | | |
| 46-50 | | 25,0% | 58,3% | 16,7% | |
| Total | 4,4% | 21,6% | 72,1% | 1,5% | 0,5% |

*Table 14. Loss or stealing of the device*

- Have you ever forgotten your device e.g. at a coffee shop?

| Age_groups | Twice | Once | Never | More | 3 times |
|---|---|---|---|---|---|
| 18-24 | 5,6% | 13,5% | 78,7% | 2,2% | |
| 25-30 | 2,7% | 10,8% | 78,4% | 2,7% | 5,4% |
| 31-35 | 9,5% | 9,5% | 81,0% | | |
| 36-40 | 13,3% | 23,3% | 63,3% | | |
| 41-45 | | 13,3% | 80,0% | 6,7% | |
| 46-50 | | 25,0% | 58,3% | 16,7% | |
| Total | 5,9% | 14,7% | 75,5% | 2,9% | 1,0% |

*Table 15. Forget the Device*

# 5 Survey Analysis Among Age Groups

### 5.1.1 Ages versus Privacy

By examining the collected data of our questionnaire, we came up with some interesting trends among the participants. Moreover, 27,1% of the participants have lost their device, at least once. In addition, they save their cash card PIN without encryption. Lastly, they give their device to others.

- In the age group 18-24 the 74,1% is careful and does not store at all important and other passwords such as Bank PINs, etc. on their mobile phone. Nevertheless, a great percentage and in specific the 23,7% does store important passwords without encryption and 82, 6% never changes the PIN of their cash card. The 2,2% stores important passwords but uses encryption. The 84,3% stores sensitive personal data such as photographs, videos etc., and 15,7% does not. The PIN question in the SIM card is enabled by the 76,4% but the 80,1% never changes it. The 23,5% has lost their device at least once and the 20,2% gives their PIN to third persons.
- In the age group 25-30 the 81% is careful and does not store important and other passwords on their mobile phone. The 16,2% does store important passwords without encryption and of this percentage nobody ever changes the PIN of their cash card. The 2,8% stores important passwords but uses encryption. The 83,8% stores sensitive personal data and 78,3% does not protect them with a PIN or a touch gesture. The 16,2% does not store sensitive data. The PIN question in the SIM card is not enabled by the 86,4% while the 91,9% never changes it. The 27% has lost their device at least once and the 26,1% gives their PIN to third persons.
- In the age group 31-40 the 35,7% stores important passwords without encryption while the rest 64,3% does not store important passwords on their device. The 78,6% never changes the PIN of their cash card. The 90,5% stores sensitive personal data and nobody protects them with a PIN or a touch gesture. The PIN question in the SIM card is enabled by the 73,8% and the 66,7% never changes it. The 38% has lost their device at least once and the 24% gives their PN to third persons.
- In the age group 41-50 the 30,6% stores important passwords without encryption while only 5,6 stores important passwords encrypted. The 88,9% never changes the PIN of their cash card. The 63,9% stores sensitive personal data and the 58,3% does not protect them with a PIN or a touch gesture. The PIN question in the SIM card is enabled by the 61,1% and the 55,5 never changes it. The 27,8% has lost their device at least once and the 27,8% gives their PIN to third persons.

Smaller age groups, as we have seen, seem to be more cautious in relation to older age groups, about the protection of their personal data. Generally, in all age groups of this category the percentage of users who do not follow any practices in order to protect their PIN and Passwords is about 19,1%. The percentage of users that gives their PIN is 22,5%. Finally, the results of this study, shows that while many smartphone users do take some security measures, a high percentage of them, 24%, still ignores potential risks.

# 6 Hypotheses of Survey

### 6.1.1 First hypothesis

*Age correlates to users' practices concerning the storage of passwords of critical applications on their mobile phone.*

To check if this hypothesis applies we use the non-parametric Kruskal – Walis test since we don't have a normal distribution and we have more than two groups to check. We examine if there is a statistically significant difference between the age groups in correlation to the variable *Store_important_password*. Initially we set the null and the alternative hypothesis:

- H0: The distribution of the variable Store_important_password is the same to all age groups.
- H1: The distribution of the variable Store_important_password is not the same to all age groups.

The results of the test are presented in the following table:

| Null Hypothesis | Test | Sig. | Decision |
|---|---|---|---|
| The distribution of the variable Store_important_password is the same to all age groups. | non-parametric Kruskal – Walis | .013 | Reject the Null Hypothesis |

*Table 16. First Hypothesis Test Summary*

Since p .013 <0.05 we reject the H0. So, we observe that the users' age concerning the storage of important passwords on their mobile phones do correlates. The median values for every age per category of answers is the following:

| Do you store important passwords on your mobile phone? (e.g. bank PINs) | | | |
|---|---|---|---|
| | **no** | **Yes, with encrypted** | **Yes, without encryption** |
| **median** | 25-30 | 18-24 | 31-35 |

*Table 17. First Hypothesis Median*

From the median values we can see that younger ages 18-30 are more careful concerning the storage of personal data on their device. The age of 31-35 is on the borderline, since it is the median in the third category (yes, without encryption) of the first case of the survey. At this age it seems that they do not store PIN and passwords on their device. From the median and above though, i.e. at ages 36- 50, as is apparent from the descriptive statistics, the users do store important password such as bank PINs, with no encryption.

### 6.1.2 Second Hypothesis

*Age correlates to the users' practices concerning the storage of sensitive personal data on their mobile (photographs / videos /voice recordings etc.).*

To check if this hypothesis applies we will use again the non-parametric Kruskal – Walis test since we don't have a normal distribution and we have more than two groups to examine. We will check if there is a statistically significant difference between the age groups in correlation to the variable Store_important_password. Initially, we set the null and the alternative hypothesis:

- H0: The distribution of the variable Store_important_password is the same in all age groups.
- H1: The distribution of the variable Store_personal_data is not the same in all age groups.

The results of the Kruskal – Walis test from the SPSS are presented in the following table:

| Null Hypothesis | Test | Sig. | Decision |
|---|---|---|---|
| The distribution of the variable Store_important_password is the same in all age groups. | non-parametric Kruskal – Walis | .009 | Reject the Null Hypothesis |

*Table 18. Second Hypothesis Test Summary*

Since there is a statistically significant difference, where p= 0.009 <0.05 we reject the H0. So we observe that the users' age in correlation to the sensitive personal data storage on their mobile (photographs / videos /voice recordings etc.) do relates.

The median values for every category of answers per age is the following:

| Do you store sensitive personal data on your mobile device? (e.g. photographs/videos etc.). | | |
|---|---|---|
| | **No** | **Yes** |
| **Median** | 25-30 | 25-30 |

*Table 19. Second Hypothesis Median*

From the median and above though, i.e. at ages 31-50, as is apparent from the descriptive statistics, the users do store sensitive personal data but the percentage gradually decreases in older ages, while it increases in the younger ones.

### 6.1.3 Third Hypothesis

*Gender correlates to the users' practices concerning the sharing of their PIN with third persons.*

To check if this hypothesis applies we will use again the non-parametric Kruskal – Walis test since we don't have a normal distribution and we have more than two groups to examine. We will check if there is a statistically significant difference between the age groups in correlation to the variable Store_important_password. Initially, we set the null and the alternative hypothesis:

- H0: The distribution of the variable Given_your_pin is the same between the two genders.
- H1: The distribution of the variable Given_your_pin is not the same between the two genders.

The results of the Kruskal – Walis test from the SPSS are presented in the following table:

| **Null Hypothesis** | **Test** | **Sig.** | **Decision** |
|---|---|---|---|
| The distribution of the variable Given_your_pin is the same between the two genders. | non-parametric Kruskal – Walis | .024 | Reject the Null Hypothesis |

*Table 20. Third Hypothesis Test Summary*

Since there is a statistically significant difference, where p= .024 <0.05 we reject the H0. We observe that there is a correlation between users' age and the Given_your_pin variable.

The median values for every category of answers per gender is the following:

| Do you give your PIN to third persons? | | |
|---|---|---|
| | yes | no |
| Median | Female | Male |

*Table 21. Third Hypothesis Median*

We observe that the median for the variable *female* is in the answer "yes", while for the variable *male* the median is in the answer "no".

We see that the gender factor affects the users' attitude on whether they give their PIN to third persons. We see that females give their PIN to third persons more easily. The percentage of users that gives their PIN is 22,5%.

## 7 Conclusions

In the results of this survey we saw the users' attitudes for the protection of their personal data and how these are affected by factors such as age. In the first hypothesis of our survey, i.e. if the users store important PIN and password on their device, we observed that there is a statistically significant correlation. Younger people, mostly of the age 18-30, seem to be more careful of ensuring their personal data. More specifically, in the age group 18-24 they avoid storing on their device bank PINs and important passwords at a percentage of 74,2%, while in the age 25-30 at a percentage of 81,1%. These age groups encrypt their data at a percentage of 13,5 and 16,2 respectively. The age of 31-35 is on the borderline, since it is the median in the third category (yes, without encryption) of the first case of the survey. At this age it seems that they do not store PIN and passwords on their device. From the median and above though, i.e. at ages 36- 50, as is apparent from the descriptive statistics, the users do

store important password such as bank PINs, with no encryption. At the same time, even though all those sensitive data are exposed, 77.9% of the respondents never change their PIN in their cash card. Generally, in all age groups of this category the percentage of users who do not follow any practices in order to protect their PIN and Passwords is about 19,1%.

In the second hypothesis of our survey we also saw that the age factor affects the users' attitude in relation to the storage of sensitive personal data on their device. We already have seen in the results of our survey, 81,9% of the users stores sensitive personal data on their mobile device. Moreover, 28% of the participants, have lost their device, at least once. Finally, they give their PIN to third persons in a percentage of 22,5% and, in the third hypothesis, we saw that females give their PIN to third persons more easily.

Answering to our main research question, which is: "Can the users' practices protect their sensitive data?", we observe that, generally, users are interested in the protection of their personal data. The younger age groups seem to take some extra steps for their protection that do not appear at older ages. But the measures taken by the users in general are not sufficient to protect them. Most of them for example protect their personal data by a PIN and they use a PIN or a touch gesture in order to protect individual elements (such as photographs, sms, telephone directory etc.) preventing access to third parties. But as it emerged from the literature review the use of current PIN-based authentication or touch gestures is problematic (Clarke and Furnell, 2005; Ahern et al. 2007; Kurkovsky and Syta 2010), (Chin et al. 2012), (Keith et al. 2013), because there is no protection after the PIN is entered. In addition, it is not sufficient since the devices are vulnerable to various attacks, such as smudge attacks (Aviv et al. 2010).

The results of this study, show that while many smartphone users do take some security measures, a high percentage 24% of them still ignores potential risks.

From all the above we firmly believe that there is a need for the amplification of users' personal data protection. Besides, a great number of studies, as the one of Clarke et al. (2002), presented their findings on the views of the subscribers concerning the need for security in mobile devices. Users were positive to alternative identification control methods, such as the fingerprint scanning and the voice recognition. In addition, the results of a survey which was also conducted by Clarke and Furnell (2005), showed that 83% of the participants are willing to accept some form of biometric Authentication on their device. Stylios et al. (2015) presented a survey where a user profile could be created through some behavioral biometrics including: the way of using the various applications, power consumption, touch gestures and guest users' habits, in order to strengthen the protection of users' sensitive personal data.

## References

Ahern, S., Eckles, D., Good, S.N, King, S., Naaman, M., Nair, R., (2007). Over-exposed?: privacy patterns and considerations in online and mobile photo sharing. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Pages 357-366. Publisher ACM New York, USA.

Androulidakis, I., Levashenko, V., Zaitseva, E. (2014). Smart phone users: Are they green users? 10th International Conference on Digital Technologies. IEEE (DT2014).

Androulidakis, I., Christou, V., Bardis, N., Stilios, I. (2009). Surveying users' practices regarding mobile phones' security features. Electrical And Computer Engineering Series, Proceedings of the 3rd WSEAS international conference. Tbilisi, Georgia, Pages: 25-30, Year of Publication: June 26, 2009, ISBN ~ ISSN:1790-5117, 978-960-474-088-8

Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M, (2010). Smudge attacks on smartphone touch screens. Proceedings of the 4th USENIX conference on Offensive technologies. pp. 1{7. USENIX Association.

Jones, B. and Heinrichs, R..L., (2012). Do business students practice smartphone security? Article in Journal of Computer Information Systems winter 2012(2):22-30, December.

Blank G, Bolsover G, Dubois E. A new privacy paradox. 2014. Working Paper, University of Oxford, Global Cyber Security Capacity Centre.

Bo, C., Zhang, L., Jung, T., Han, J., Li, X.-Y., Wang, Y. (2014). Continuous user identification via touch and movement behavioral biometrics. Performance Computing and Communications Conference (IPCCC), 2014 IEEE International. pp. 1{8.IEEE (2014).

Chin, E., Porter Felt, A., Sekar, V., Wagner, D., (2012). Measuring user confidence in smartphone security and privacy. Proceedings of the Eighth Symposium on Usable Privacy and Security. Article No. 1. ISBN: 978-1-4503-1532-6NY, Publisher ACM New York, USA.

Clarke N., L., Furnell, S., M., (2002). Acceptance of Subscriber Authentication Methods For Mobile Telephony Devices. Computers & Security Volume 21, Issue 3, 1 June 2002, Pages 220–228.

Clarke N., L., Furnell, S., M., (2005). Authentication of users on mobile telephones – A survey of attitudes and practices. Computers & Security 24, 519e527, Elsevier.

Dillman, D. A., (1999) Mail and Internet Surveys: The Tailored Design Method, John Wiley & Sons, 2nd edition, November 1999.

Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. Information Forensics and Security, IEEE Transactions on. 8, 136{148 (2013).M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

Karatzouni, S., Furnell, S.M., Clarke, N.L. and Botha, R.A., (2007). Perceptions of User Authentication on Mobile Devices. In Proceedings of the 6th Annual ISOnEworld Conference, April 11-13, 2007, Las Vegas, NV.

Keith, J.M., Thompson, S.C., Hale, J., Benjamin Lowry, P., Greer, C., (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. International Journal of Human-Computer Studies Volume 71, Issue 12, December 2013, Pages 1163–1173. ELSEVIER.

Kurkovsky, S. and Syta, E., (2010). Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. 2010 IEEE International Symposium on Technology and Society (ISTAS). Conference Location: Wollongong, NSW. Page(s): 441 - 449. Print ISBN: 978-1-4244-7777-7.

Miltgen CL, Peyrat-Guillard D. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. Eur J Inform Syst 2014;23(2):103–25.

Stylios, I., Chatzis, P. S., Thanou, O., Kokolakis, S, (2015). Mobile Phones & Behavioral Modalities: Surveying users' practices. International IEEE Conference TELFOR 2015, November 2015, SAVA Center, Belgrade, Serbia.